IN THE DRAWINGS:

Please replace originally filed Fig. 6A with replacement Fig. 6A attached hereto.

REMARKS

Claims 1-65 are pending in this application. By this Amendment, claims 1-3, 5, 7, 8, 10-13, 15, 18, 19, 22-26, 29-36, 38, 40, 42-45, 47, 49-50, 52-56, and 59-61 are amended to further clarify the recited subject matter, and new claims 62-65 are added. Originally filed Fig. 6A is replaced with new Fig. 6A. The above-indicated amendments are supported by the original disclosure and no new matter is added by these amendments. Reconsideration in view of the following remarks is respectfully requested.

I. PRIOR ART REJECTIONS - 35 U.S.C. §102

A. CLAIMS 1-4, 30-31, AND 34-37 ARE PATENTABLE OVER BISBEE ET AL.

The Office Action rejected claims 1-4, 30-31, and 34-37 under 35 U.S.C. §102(b) as being unpatentable over Bisbee et al. (U.S. Patent No. 5,748,738, hereinafter "Bisbee"). The Applicant traverses the rejection because Bisbee fails to teach or suggest all of the features recited in the rejected claims.

i. CLAIMS 1-4 ARE PATENTABLE OVER BISBEE

For example, Bisbee fails to teach or suggest a method for creating a unique authoritative electronic record, comprising "receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of a combination of both the electronic record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; and, storing the record with the prepended receipt and the appended identifying information and supplemental information as the unique authoritative record in the repository" (emphasis added), as recited in claim 1.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee)

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally

signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Therefore, Bisbee fails to teach or suggest and, in fact, teaches away from a method for creating a unique authoritative electronic record, comprising "receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of a combination of both the electronic record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; and, storing the record with the prepended receipt and the appended identifying

information and supplemental information as the unique authoritative record in the repository" (emphasis added), as recited in claim 1.

Accordingly, Applicant respectfully submits that independent claim 1, is patentable over Bisbee. Likewise, claims 2-4, which depend, either directly or indirectly, from independent claim 1, are also patentable over Bisbee for the reasons discussed above plus the additional feature(s) they recite. Thus, claims 1-4 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §102 is respectfully requested.

ii. CLAIMS 30-31 ARE PATENTABLE OVER BISBEE

For example, Bisbee fails to teach or suggest a computer readable medium for storing a program that allows a user to "receive, and digitally sign a copy of an electronic record that is stored in a remote location, wherein the program provides for the user to: receive a proper subset of the electronic record, wherein the proper subset of the electronic record allows the user to view, store and print the record, and when the user is ready, to: sign the electronic record, wherein the program requests and receives at least a partially completed message digest of the electronic record, wherein the partial message digest is related to the complement of the proper subset of the electronic record, and the user then uses the partial message digest, the proper subset, and identifying information, to complete the computation of the message digest of the electronic record to be signed, and the user then uses the completed message digest and a private key to digitally sign the record" (emphasis added), as recited in claim 30.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature".

However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Therefore, Bisbee fails to teach or suggest and, in fact, teaches away from a computer readable medium for storing a program that allows a user to "receive, and digitally sign a copy of an electronic record that is stored in a remote location, wherein the program provides for the user to: receive a proper subset of the electronic record, wherein the proper subset of the electronic record allows the user to view, store and print the record, and when the user is ready, to: sign the electronic record, wherein the program requests and receives at least a partially completed message digest of the electronic record, wherein the partial message digest is related to the complement of the proper subset of the electronic record, and the user then uses the partial message digest, the proper subset, and identifying information, to complete the computation of the message digest of the electronic record to be signed, and the user then uses the completed message digest and a private key to digitally sign the record" (emphasis added), as recited in claim 30.

Accordingly, Applicant respectfully submits that independent claim 30, is patentable over Bisbee. Likewise, claim 31, which depends, either directly or indirectly, from independent claim 30, is also patentable over Bisbee for the reasons discussed above plus the additional feature(s) it recites. Thus, claims 30-31 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §102 is respectfully requested.

iii. CLAIMS 34-37 ARE PATENTABLE OVER BISBEE

For example, Bisbee fails to teach or suggest an apparatus for creating and storing a unique authoritative record, comprising "at least one server, connected to a network, that stores and executes software for receiving a record in a secure environment wherein the secure environment is created by the server and the software; wherein the software provides for: generating identifying information; generating a receipt, wherein the receipt includes a digital signature of the combination of the authoritative record and the appended identifying information; generating supplemental information that includes a provable representation of

the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; and, storing the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record in the secure environment" (emphasis added), as recited in claim 34.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee)

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by

itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Therefore, Bisbee fails to teach or suggest and, in fact, teaches away from an apparatus for creating and storing a unique authoritative record, comprising "at least one server, connected to a network, that stores and executes software for receiving a record in a secure environment wherein the secure environment is created by the server and the software; wherein the software provides for: generating identifying information; generating a receipt, wherein the receipt includes a digital signature of the combination of the authoritative record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; and, storing the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record in the secure environment" (emphasis added), as recited in claim 34.

Accordingly, Applicant respectfully submits that independent claim 34 is patentable over Bisbee. Likewise, claims 35-37, which depend, either directly or indirectly, from independent claim 34, are also patentable over Bisbee for the reasons discussed above plus the additional feature(s) they recite. Thus, claims 34-37 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §102 is respectfully requested.

II. PRIOR ART REJECTIONS - 35 U.S.C. §103

A. CLAIMS 5-29, 32-33, AND 38-61 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

The Office Action rejected claims 5-29, 32-33, and 38-61 under 35 U.S.C. §103(a) as being unpatentable over Bisbee et al. (U.S. Patent No. 5,748,738, hereinafter "Bisbee") in view of Vanstone (U.S. Patent No. 6,212,281, hereinafter "Vanstone"). The Applicant traverses the rejection because the combined teachings of Bisbee and Vanstone fail to teach all of the features recited in the rejected claims.

i. CLAIMS 5-10 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising "receiving a

request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; computing a complement of the proper subset; sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest, the complement of the proper subset, and identifying information; and, creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in claim 5.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to

obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record. Thus, Bisbee fails to teach the claimed subject matter of original claim 5.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a

hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising "receiving a request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; computing a complement of the proper subset; sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest, the complement of the proper subset, and identifying information; and, creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in claim 5, and fail to overcome the deficiencies of Bisbee.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising "receiving a request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; computing a complement of the proper subset; sending the partial message digest and at least the complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest, the complement of the proper subset, and identifying information; and,

creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in claim 5.

Therefore, Applicant respectfully submits that independent claim 5 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 6-10 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 5, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 5-10 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

ii. CLAIMS 11-17 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising "receiving a record in a secure environment, wherein the secure environment is connected to a network and comprises at least one server that stores and executes software; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of a combination of the record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; storing the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record; receiving a request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest, the complement of the proper subset, and other identifying information; creating a digital signature with the use of the message digest and a private key; transmitting at least the digital signature and the other identifying information to the secure environment; validating the digital signature in the secure environment, and upon affirmative validation; revising the authoritative record with the digital signature and other information to create a revised authoritative record" (emphasis added), as recited in claim 11.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record. Thus, Bisbee fails to teach the claimed subject matter of original claim 11.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising "receiving a record in a secure environment, wherein the secure environment is connected to a network and comprises at least one server that stores and executes software; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of a combination of the record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; storing the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record; receiving a request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest, the complement of the proper subset, and other identifying information; creating a digital signature with the use of the message digest and a private key; transmitting at least the digital signature and the other identifying information to the secure environment; validating the digital signature in the secure environment, and upon affirmative validation; revising the authoritative record with the digital signature and other information to create a revised authoritative record" (emphasis added), as recited in claim 11, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising "receiving a record in a secure environment, wherein the secure environment is connected to a network and comprises at least one server that stores and executes software; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of a combination of the record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; storing the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record; receiving a request to sign the authoritative record; computing a partially completed message digest of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to a remote location; completing the computation of the message digest, at the remote location, using the partial message digest, the complement of the proper subset, and other identifying information; creating a digital signature with the use of the message digest and a private key; transmitting at least the digital signature and the other identifying information to the secure environment; validating the digital signature in the secure environment, and upon affirmative validation; revising the authoritative record with the digital signature and other information to create a revised authoritative record" (emphasis added), as recited in claim 11.

Therefore, Applicant respectfully submits that independent claim 11 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 12-17 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 11, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 11-17 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

iii. CLAIMS 18-29 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, comprising "receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially complete message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce a digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature,

a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 18.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic

disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest

of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, comprising "receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in

the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially complete message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce a digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 18, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a

copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, comprising "receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially complete message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce a digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature

information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 18.

Therefore, Applicant respectfully submits that independent claim 18 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 19-29 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 18, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 18-29 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

iv. CLAIMS 32-33 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a method for digitally signing an electronic record received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising "receiving the second portion of the electronic record from the secure environment, wherein the second portion allows a user to view, print or store the electronic record; receiving a partially complete message digest of the electronic record from the secure environment wherein the partial message digest is related to the first portion of the electronic record; completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information; and, creating a digital signature of the electronic record using the message digest and a private key" (emphasis added), as recited in claim 32.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally

signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by

itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a method for digitally signing an electronic record received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising "receiving the second portion of the

electronic record from the secure environment, wherein the second portion allows a user to view, print or store the electronic record; receiving a partially complete message digest of the electronic record from the secure environment wherein the partial message digest is related to the first portion of the electronic record; completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information; and, creating a digital signature of the electronic record using the message digest and a private key" (emphasis added), as recited in claim 32, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a method for digitally signing an electronic record received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising "receiving the second portion of the electronic record from the secure environment, wherein the second portion allows a user to view, print or store the electronic record; receiving a partially complete message digest of the electronic record from the secure environment wherein the partial message digest is related to the first portion of the electronic record; completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information; and, creating a digital signature of the electronic record using the message digest and a private key" (emphasis added), as recited in claim 32.

Therefore, Applicant respectfully submits that independent claim 32 is patentable over Bisbee in view of Vanstone. Likewise, dependent claim 33 is also patentable over Bisbee in view of Vanstone by virtue of its dependence from claim 32, for the reasons discussed above, and for the additional feature(s) it recites. Thus, claims 32 and 33 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

v. CLAIMS 38-42 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a system for obtaining a digital signature on an authoritative record that is stored in a secure environment, comprising "a server that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes at least of portion of the software, wherein the software provides for: receiving a request from the remote location to sign the authoritative record; computing a partially completed message digest at the secure environment, of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and identifying information; and, creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in claim 38.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest

of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record. Thus, Bisbee fails to teach the claimed subject matter of original claim 38.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a system for obtaining a digital signature on an authoritative record that is stored in a secure environment, comprising "a server that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes at least of portion of the software, wherein the software provides for: receiving a request from the remote location to sign the authoritative record; computing a partially completed message digest at the secure environment, of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and identifying information; and, creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in claim 38, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a system for obtaining a digital signature on an authoritative record that is stored in a secure environment, comprising "a server that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes at least of portion of the software, wherein the software provides for: receiving a request from the remote location to sign the authoritative record; computing a partially completed message digest at the secure environment, of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and identifying information; and, creating a digital signature with the use of the message digest and a private key" (emphasis added), as recited in claim 38.

Therefore, Applicant respectfully submits that independent claim 38 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 39-42 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 38, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 38-42 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

vi. CLAIMS 43-48 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a system for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising "at least one server, connected to a network, that stores and executes software that creates a secure environment and at least one computer at a remote location that stores and executes at least a portion of the software, wherein the software provides for: receiving a record in the secure environment; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of the combination of the authoritative record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record;

appending the identifying information and the supplemental information to an ending of the record; storing, in the secure environment, the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record; receiving a request, from the remote location, to sign the authoritative record; computing a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and identifying information; creating a digital signature with the use of the message digest and a private key; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; validating the digital signature in the secure environment, and upon affirmative validation; revising the authoritative record with the digital signature and other information to create a revised authoritative record" (emphasis added), as recited in claim 43.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way

that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a system for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising "at least one server, connected to a network, that stores and executes software that creates a secure environment and at least one computer at a remote location that stores and executes at least a portion of the software, wherein the software provides for: receiving a record in the secure environment; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of the combination of the authoritative record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; storing, in the secure environment, the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record; receiving a request, from the remote location, to sign the authoritative record; computing a partially completed message digest, at the secure environment, of the authoritative record,

wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and identifying information; creating a digital signature with the use of the message digest and a private key; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; validating the digital signature in the secure environment, and upon affirmative validation; revising the authoritative record with the digital signature and other information to create a revised authoritative record" (emphasis added), as recited in claim 43, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a system for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising "at least one server, connected to a network, that stores and executes software that creates a secure environment and at least one computer at a remote location that stores and executes at least a portion of the software, wherein the software provides for: receiving a record in the secure environment; generating identifying information; generating a receipt, wherein the receipt includes a digital signature of the combination of the authoritative record and the appended identifying information; generating supplemental information that includes a provable representation of the receipt; prepending the receipt to a beginning of the record; appending the identifying information and the supplemental information to an ending of the record; storing, in the secure environment, the record with prepended receipt and appended identifying information and supplemental information as the unique authoritative record; receiving a request, from the remote location, to sign the authoritative record; computing a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to a proper subset of the authoritative record; sending the partial message digest and at least a complement of the proper subset of the authoritative record to the remote

location; completing the computation of the message digest, at the remote location, using the partial message digest and the complement of the proper subset, and identifying information; creating a digital signature with the use of the message digest and a private key; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; validating the digital signature in the secure environment, and upon affirmative validation; revising the authoritative record with the digital signature and other information to create a revised authoritative record" (emphasis added), as recited in claim 43.

Therefore, Applicant respectfully submits that independent claim 43 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 44-48 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 43, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 43-48 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

vii. CLAIMS 49-59 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest a system for creating and validating at least one digital signature on an electronic authoritative record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the system comprising "at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for: receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning

of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a person at the remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce the digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 49.

In contrast, as discussed above, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally

signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

According to Bisbee, the combination of these functions, in conjunction with a protected audit trail, can be used at a future date to prove conclusively that a party initiated a transaction. In particular, Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the

document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee merely discloses appending certificate(s), digital signature(s), and date and time stamp(s), to an electronic document.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from a system for creating and validating at least one digital signature on an electronic authoritative record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic

authoritative record's integrity, the system comprising "at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for: receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a person at the remote location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce the digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature

information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 49, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) a system for creating and validating at least one digital signature on an electronic authoritative record that is maintained in a secure environment, wherein a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the system comprising "at least one server, connected to a network, that stores and executes software that creates the secure environment and at least one computer at a remote location that stores and executes a portion of the software, wherein the software provides for: receiving an electronic record in the secure environment; generating at least some identifying information; generating at least some first information comprising a receipt of the electronic record by the secure environment; defining a beginning information as all information prepended to a beginning of the record and comprising the first information; generating at least some second information comprising at least a provable representation of the first information, wherein the provable representation of the first information is mathematically related to the first information; defining an ending information as all information appended to an end of the record and comprising the identifying information and the second information; creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record; storing the authoritative record in the secure environment; making a perceivable copy of the authoritative record by copying only the electronic record and the ending information; transmitting the perceivable copy of the authoritative record to a person at the remote

location; receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record by: generating a partially completed message digest, at the secure environment, of the authoritative record, wherein the partial message digest is related to the beginning information; transmitting the partial message digest from the secure environment to the remote location, completing a message digest of the authoritative record at the remote location with the use of the partial message digest, the perceivable copy, and other identifying information; and, creating a digital signature at the remote location using the message digest and a private key to produce the digital signature of the authoritative record; transmitting at least the digital signature and the other identifying information from the remote location to the secure environment; receiving the digital signature and the other identifying information in the secure environment; validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the combination of the authoritative record and the received identifying information in the secure environment, and upon affirmative validation of the digital signature; generating a revised authoritative record by prepending digital signature information comprising at least the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising at least the received identifying information and a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information; and, storing the revised authoritative record in the secure environment" (emphasis added), as recited in claim 49.

Therefore, Applicant respectfully submits that independent claim 49 is patentable over Bisbee in view of Vanstone. Likewise, dependent claims 50-59 are also patentable over Bisbee in view of Vanstone by virtue of their dependence, either directly or indirectly, from claim 49, for the reasons discussed above, and for the additional feature(s) they recite. Thus, claims 49-59 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

viii. CLAIMS 60-61 ARE PATENTABLE OVER BISBEE IN VIEW OF VANSTONE

For example, Bisbee fails to teach or suggest an apparatus for digitally signing an electronic record that is received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising "a computer that stores and

executes software, wherein the software provides for: receiving the second portion of the electronic record from the secure environment, wherein the second portion allows a user to view, print or store the electronic record; receiving a partially completed message digest of the electronic record from the secure environment, wherein the partial message digest is related to the first portion of the electronic record; completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information; and, creating a digital signature of the electronic record using the message digest and a private key" (emphasis added), as recited in claim 60.

In contrast, Bisbee merely discloses a document authentication system that uses an Authentication Center to provide an audit or evidence trail from the original execution of an executed, encrypted, or sealed document through all subsequent transmissions. (See Col. 5, lines 34-38 of Bisbee).

In Bisbee, each transaction and document is authenticated by transmission to the Authentication Center from a Transfer Agent's terminal. The Transfer Agent provides the document in digital form to the Transfer Agent's Token. The digital document is digitally signed and/or encrypted by the document authentication system Token, and the digitally signed and/or encrypted version is communicated to the Authentication Center electronically (including, dispatching a diskette containing the document). (See Col. 6, lines 14-30 of Bisbee)

The Authentication Center verifies the identity of the Transfer Agent and the authenticity of the documents, and appends a digital signature and a date and time stamp to the document, thereby establishing each transaction in a manner which can not be repudiated. (See Col. 6, lines 31-35 of Bisbee)

Bisbee claims to provide authentication of a document in a way that prohibits an originator from denying that the document originated with that originator, and provides irrevocable proof of authenticity. (See Col. 6, lines 35-42 of Bisbee)

The authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center in any convenient form, such as on optical and/or magnetic disks. Once a transaction is completed and the digitally signed and/or encrypted document or documents are transmitted and authenticated by the Authentication Center, any authorized party can access the Authentication Center through an electronic device such as a modem to obtain or further transmit an authenticated document. All transmissions of electronic documents from the originator are made to the Authentication Center, which provides

authentication and stores the authenticated documents for transmission to and on behalf of authorized parties. (See Col. 6, lines 43-57 of Bisbee)

As further described in Bisbee, the steps of digitally signing an electronic document and validating the digital signatures operate on an electronic document that has one or more digital signatures and the certificate(s) of the signatory(s) appended to it. (See Col. 10, lines 50-57 of Bisbee)

The signature validation step comprises decrypting the message digest appended to the document, re-hashing the document to generate another message digest, and comparing the resulting message digest to the decrypted message digest. The public signature/verification key found in the certificate signed by the Certification Authority and appended to the document is used for decrypting the appended message digest. If the two message digest values agree, the identity of the individual named in the certificate can be asserted as the signatory of the document, or other information object, and the integrity of the document is confirmed and guaranteed. An Authentication Center attests to this result by itself digitally signing the document. (See Fig. 9 and Col. 10, line 50 - Col. 11, line 12 of Bisbee)

Additionally, the Office Action states that "Vanstone discloses generating a hash (message digest) of a part (partial) of a document". However, it should be appreciated that the hash of a part of a document is not the same as part of a hash of a document. As disclosed in Vanstone, full message digests of parts of a document are utilized. This is not the same as a partially-completed message digest of a document. Thus, the "hash of part of a document" is not equivalent to a partial hash.

Thus, Bisbee discloses forwarding the actual electronic document for review and execution and then, upon receipt of the executed electronic document, authenticating the received electronic document with the appended electronic signature.

Furthermore, as indicated in the Office Action, Bisbee fails to teach or suggest computing, at the secure location and sending, to a remote location, the partial message digest of a proper subset of the authoritative record, along with the complement of the proper subset of the authoritative record.

The inclusion of Vanstone fails to overcome the deficiencies of Bisbee. Vanstone merely discloses a digital signature protocol that "generates a signature component using a hash of an encrypted message. The component and encrypted message form a signature pair that is forwarded to a recipient. The encryption message is used to retrieve the encryption

key at the recipient and authenticate information in the message. The signature pair may be applied to a data carrier as a bar code for use in mail delivery services. By utilizing a hash of the message, a reduced message length is achieved as individual signatures are not required for each component of the message." (See Abstract of Vanstone)

As further described in Vanstone, it is usual for a "message to include some redundancy, e.g. by repeating part or in some cases all of the message. This provides the function of the message that confirms authenticity. The redundancy provides a pattern within the recovered message that would be expected by the recipient. Any tampering with the message would be unlikely to produce such a pattern when decrypted and so would be readily detected." (See Col. 1, Lines 47-54 of Vanstone)

Thus, the teachings of Vanstone teach away from an apparatus for digitally signing an electronic record that is received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising "a computer that stores and executes software, wherein the software provides for: receiving the second portion of the electronic record from the secure environment, wherein the second portion allows a user to view, print or store the electronic record; receiving a partially completed message digest of the electronic record from the secure environment, wherein the partial message digest is related to the first portion of the electronic record; completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information; and, creating a digital signature of the electronic record using the message digest and a private key" (emphasis added), as recited in claim 60, and fail to overcome the deficiencies of Bisbee.

In fact, if the document authentication system of Bisbee were to be modified to include the digital signature protocol taught in Vanstone, the resulting system would not require individual signatures for each component of the electronic document.

Since the teachings of Vanstone fail to overcome the deficiencies of Bisbee, the teachings of Bisbee and Vanstone, either alone or in combination, fail to teach or suggest (and actually teach away from) an apparatus for digitally signing an electronic record that is received from a secure environment, wherein the electronic record consists of a first portion and a second portion, comprising "a computer that stores and executes software, wherein the software provides for: receiving the second portion of the electronic record from the secure environment, wherein the second portion allows a user to view, print or store the electronic record; receiving a partially completed message digest of the electronic record from the

secure environment, wherein the partial message digest is related to the first portion of the electronic record; completing the message digest of the electronic record using the partial message digest, the second portion, and identifying information; and, creating a digital signature of the electronic record using the message digest and a private key" (emphasis added), as recited in claim 60.

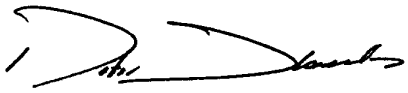
Therefore, Applicant respectfully submits that independent claim 60 is patentable over Bisbee in view of Vanstone. Likewise, dependent claim 61 is also patentable over Bisbee in view of Vanstone by virtue of its dependence from claim 60, for the reasons discussed above, and for the additional feature(s) it recites. Thus, claims 60 and 61 are allowable and withdrawal of the rejection of these claims under 35 U.S.C. §103 is respectfully requested.

CONCLUSION

Based on the foregoing amendments and remarks, Applicant respectfully submits that claims 1-65 are directed to allowable subject matter and that the application is in condition for allowance. Accordingly, prompt reconsideration and allowance of the application with these claims is respectfully requested.

However, if the Examiner believes there is anything further necessary to place this application in better condition for allowance, Applicant requests the Examiner telephone Applicant's undersigned representative at the number listed below.

Respectfully submitted,



Peter A. Shaddock II
Registration No. 44,331

Date: FEB. 28, 2006

Bowman Green Hampton & Kelly, PLLC
501 Independence Parkway, Suite 201
Chesapeake, VA 23320-5173

Telephone: (757) 548-2323
Fax: (757) 548-2345
E-mail: pshaddock@bghklaw.net